



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/745,461	12/21/2000	John E. Schier	062891 . 0490	2553

7590 01/12/2005
Kevin J. Meek, Esq.
Baker Botts L.L.P.
2001 Ross Avenue
Dallas, TX 75201

EXAMINER

HO, THOMAS M

ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 01/12/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/745,461

Applicant(s)

SCHIER, JOHN E.

Examiner

Thomas M Ho

Art Unit

2134

-- The MAILING DATE of this communication appears on the cover sheet with the corresponding address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 7/30/04.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-10 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-10 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. Claims 1-10 are pending.

Response to Arguments.

2. Applicant's arguments filed 7/30/2004 have been fully considered but they are not persuasive.

Applicant(paragraph 1, page 7) has argued:

"...the access code of Pegg, which is generated from the access key and the dynamic variables, is not "used as an index into an encryption selection table" as recited in Applicant's claim 1. Pegg discloses that it is the valid account ID that is "used to locate the users corresponding data file containing the proper selected cipher algorithm index 122 and the user's access key 114."

While the Examiner agrees that the account ID is an element used in indexing the algorithm. It nevertheless remains that the access key of the user plays a key role in the selection of the algorithm. The general consensus of the term indexing is something that serves to guide, point out, or otherwise facilitate reference.

in·dex  **Pronunciation Key** (ĩn 'dĕks')

n. pl. **in·dex·es** or **in·di·ces** (-dĩ-sĕz')

Something that serves to guide, point out, or otherwise facilitate reference,

Source: The American Heritage® Dictionary of the English Language, Fourth Edition

Pegg (Column 4, lines 15-20) states “an account access administrator assigns each user a static account ID 116 and a static access key 114 which uniquely identifies the user to an appropriate access system.” Once the user is uniquely identified, the proper algorithm may be selected as conceded by Applicant’s (paragraph 1, page 7) referencing of Pegg(Column 5, lines 41-45)

In light of the definition of “index” and indexing, the Examiner has interpreted that static access key, is indeed *used as an index* into an encryption algorithm table, because it serves to guide, or facilitate reference to the algorithm table in that it is used(along with the account ID) to unique identify the user to the appropriate access system (Pegg Column 4, lines 15-20), which then is turn is used to acquire the appropriate algorithm.

Applicant (paragraph 2, page 7) has cited as a further example:

“Applicant respectfully submits that Pegg does not disclose, teach, or suggest “encrypting the data message using the encryption method associated with the table key value” or transmitting the encrypted data message over a data communication network,” as recited in Applicant’s Claim 1. In fact, and as discussed above, the access codes 123 and 124 generated by the user and the authorization center, respectively are merely compared to determine whether a match exists”

The Examiner has interpreted the encryption or encipherment of the data message to be the algorithm that is used to masque the original access key with regards to future attempts by the user to access the system. As previously cited by Examiner Pegg (Column 4, lines 48-52), the purpose of the algorithm is to substantially disguise the user's access key. In this sense, this data message containing the user's access key is encrypted using the user's previously selected algorithm.

This message is also transmitted over a data communication network to the user.

For these reasons, the rejection of 5/19/04 stands.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-2,4-6, 8-10 are rejected under 35 U.S.C. 102(b) as being anticipated by Pegg.

In reference to claim 1:

Pegg discloses a method for communicating a data message comprising:

- Selecting a table key value, the key value being a function of a periodic key value and a public variable key value, where the periodic key value and the public variable key value is second cipher key and the first cipher key. (Column 2, lines 43-63) & (Pegg Column 4, lines 15-20),
- the encryption selection table specifying at least one of a plurality of encryption methods to be used to encrypt a data message, where an enciphering algorithm selection table is disclosed (Figure 1), and the plurality of encryption methods is the plurality of enciphering algorithms.
- Encrypting the data message using the indicated encryption method, where the chosen method encrypts the access codes. (Column 4, lines 48-52) & (Pegg Column 4, lines 15-20).
- Transmitting the encrypted data message, where the data message is transmitted by the user and transmitted to the user. (Figure 2a, step 215)

In reference to claim 2:

Pegg discloses the method of claim 1 and further comprising:

- Receiving a periodic key value and a public variable key value at a communication device storing the encryption selection table, where the first cipher key and the second cipher key is received at the server in order to compute the access code. (Column 2, lines 40-50)
- Calculating the table key value from the public variable key value and the periodic key values, where the access code is generated based on the values of the

first cipher key and the second cipher key. (Column 2, lines 40-50) & (Column 4, lines 29-34)

In reference to claim 4:

Pegg(Column 2, lines 45-50) discloses the method of claim 1 wherein the periodic key value comprises a predetermined number agreed upon between a transmitter and a recipient of the data message, where the periodic key values is the second cipher key, or the PIN number, predetermined and agreed upon by both parties.

In reference to claim 5:

Pegg(Column 2, lines 45-50) discloses the method of claim 1 wherein the public variable key value comprises a numeric value which is variable and which is available to both the recipient and the transmitter of the data message, wherein the public variable key is a first cipher key such as the current Dow Jones Industrial Average.

In reference to claim 6:

Pegg discloses a data communication device operable to transmit and receive data messages to and from a data communication network, the device comprising:

- A central processing unit operable to interface with a user of the device through a user interface, where the central processing unit is the CPU in any computer system such as that frequently used to implement an ATM system. (Figure 3)
- An encryption decryption engine under the control of the central processing unit and operable to execute a plurality of encryption programs, each of the

encryption programs being different than the remainder of the plurality and each of the encryption programs operable to receive a message and to output an encrypted message, where each of the encryption algorithms disclosed may be executed by a CPU running the algorithms and where each of them receive a message consisting of keys and output a message code (Column 4, lines 29-40), substantially disguising or encrypting the previous access key (Column 4, lines 48-52), and decrypting the operator by recomputing the enciphered access key to see if it matches. (Column 5, lines 3-8)

- An encryption selection table accessible using a key value, the encryption selection table specifying at least one of the plurality of encryption programs to be used for each key value, where an enciphering algorithm selection table is disclosed (Figure 1), and where this encryption selection table is accessible using a key value in that it is used to uniquely identify the individual (Pegg Column 4, lines 15-20), and once the user is identified, the proper algorithm is selected from the table. (Column 5, lines 40-45)

In reference to claim 8:

Pegg (Column 2, lines 40-50) discloses the device of claim 6 wherein the key value comprises a table key value and further comprising a user interface operable to prompt a user of the device and to receive a public variable key value and a periodic key value, the table key value calculated as a function of at least one or both of the public variable key value and the periodic key value, where the user is prompted to enter the necessary

information (Figure 2a), consisting of the first and second cipher keys. (Column 2, lines 40-50)

In reference to claim 9:

Pegg (Column 2, lines 45-50) discloses the device of claim 8 wherein the public variable key value comprises a numeric value which is variable and which is available to both the recipient and the transmitter of the data message, wherein the public variable key is a first cipher key such as the current Dow Jones Industrial Average.

In reference to claim 10:

Pegg (Column 2, lines 45-50) discloses the device of claim 8 wherein the periodic key value comprises a predetermined number agreed upon between a transmitter and a recipient of the data message, where the periodic key values is the second cipher key, or the PIN number, predetermined and agreed upon by both parties.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 3 and 7 are rejected under 35 U.S.C. 103(a) as being unpatentable over Pegg.

In reference to claim 3:

Pegg(Figure 2b) discloses:

Selecting a second encryption method also specified by the table key value from the encryption selection table, where a second selection method may be determined by selecting a different algorithm in the algorithm selection table.

Pegg however fails to explicitly disclose:

Encrypting the data message a second time using the second encryption method prior to transmitting the encrypted message.

The examiner takes official notice that second encrypting a message using a second encryption algorithm in succession or serially was well known in the art at the time of invention.

Well known examples are 3-DES, or Finley(US patent 5,742,686), Moore(US patent 5,343,527), or Campinos(US patent 6,091,818) or Leppek, US patent (5,933,501)

Furthermore, Finley(Column 2, lines 34-40) even teaches that one of that advantages of serially/multiply encrypting data when encryption methods are dynamically selected is advantageous.

“Even if a hacker knows every encryption code and password that the user could use, the hacker has no way of knowing which encryption codes will be randomly selected or the order of repetition count in which they will be executed”

Leppek discloses the practice of using a database of multiple algorithms and performing a plurality of encryptions to increase security. In regards to the advantages of this, Leppek discloses:

“From the foregoing, it will readily be appreciated that subjecting the data to successively different encryption operators will produce a compound-encrypted data stream having no readily discernable encryption footprint. Therefore, even if a skilled data communications usurper is in possession of a decryption key for each of the encryption operators A, B and C of which the five member compound encrypted data stream of the present example is comprised, there is a very low likelihood that he would be able to recognize the characteristics of any individual encryption operator in the transmitted data stream.”

It would have been obvious to one of ordinary skill in the art at the time of invention to second encrypt the data using a selected algorithm from an algorithm table before transmitting it to another party because it would provide an extra layer of security in the encryption.

Claim 7 is rejected for the same reasons as claim 3.

Conclusion

5. THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of the final action and the advisory action is not mailed under after the end of the THREE-MONTH shortened statutory period, then the

shortened statutory period will expire on the date the advisory action is mailed, and any extension pursuant to 37 CFR 1.136(A) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

6. Any inquiry concerning this communication from the examiner should be directed to Thomas M Ho whose telephone number is (571)272-3835. The examiner can normally be reached on M-F from 9:30 AM - 6:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory A. Morse can be reached on (571)272-3838.

The Examiner may also be reached through email through Thomas.Ho6@uspto.gov


Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (571)272-2100.

General Information/Receptionist Telephone: 571-272-2100 Fax: 703-872-9306

Customer Service Representative Telephone: 571-272-2100 Fax: 703-872-9306

January 6th, 2005,

TMH


GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100